



(/)

iboss

SECURE WEB GATEWAY
PLATFORM



OVERVIEW

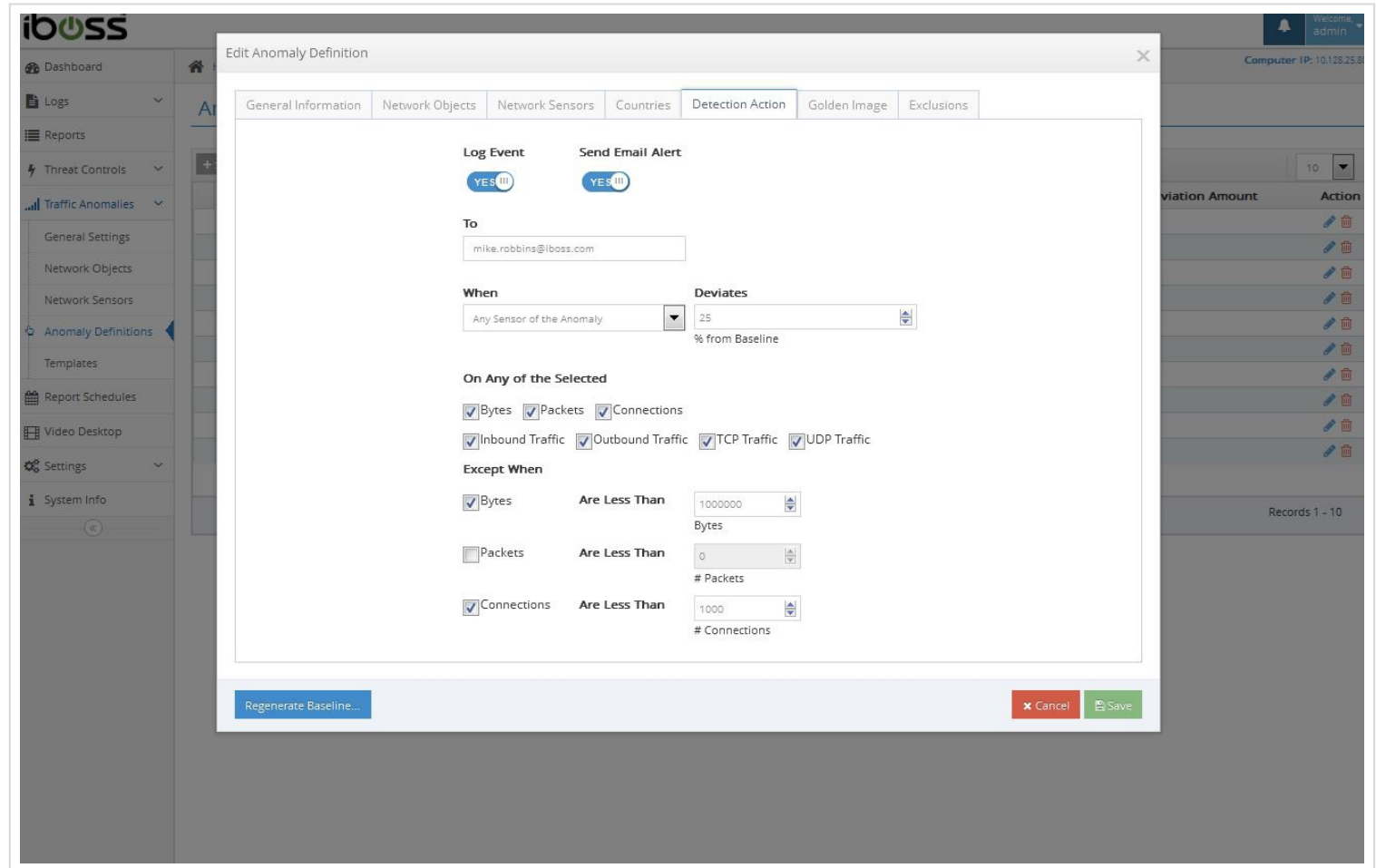
TECHNOLOGIES

ARCHITECTURE

Network Anomaly Detection

Finds infections hijacking data 100X faster

The iboss Secure Web Gateway Platform's exclusive network anomaly detection exposes the most evasive signatureless malware, even after it's made it past your sandbox. Once a problem is pinpointed, you immediately receive real-time email alerts and your data is contained, before it is hijacked. Our technology takes only minutes to deploy and provides 24/7 peace of mind, without requiring you to reconfigure the entire network.



Detect command and control callbacks

Scans across DNS, IP other protocols

The iboss Secure Web Gateway Platform leverages visibility across all TCP and UDP ports to scan for evasive threats on hidden ports and protocols include those using DNS, IP, SSH, IMAP, POP and many others. It also scans for command and control callbacks and thwarts attacks such as network probes and port scans.

Machine Details

Clear Infection
Clear High Risk
Add/Show Notes (10)
Download Detailed Report

General Info for KJOHNSON_COMP (10.128.16.97): This Machine is **Infected** and exhibits **High Risk Behavior** (Malware Access)

Security Group:

Current Infection Status: **INFECTED**

User at Infection Time: kjohnson
Infection Incidents: 7
Dwell Time: Avg: 596.5 hrs / Total: 5,563.9 hrs
First Callback Detection: 06/10/2015 12:08 PM
First Callback Dest: 56.18.19.150
First Callback Signature: bronetbro.com
Last Callback Detection: 07/02/2015 5:34 PM
Last Callback Dest: 156.153.226.92
Last Callback Signature: vperedzaddos.com

Risk Status: **HIGH**

Risky Behaviors: Malware Access
Malware Access Count: 4256
User at Malware Risk Event: kjohnson
First Malware Detection: 02/03/2015 8:39 AM
Last Malware Detection: 07/02/2015 5:34 PM
Last Malware Dest. IP: 156.153.226.92
Last Malware Dest. URL: q47m1u3.com
First Malware Dest IP: 27.79.158.234

Key Events
Infection Callbacks
Malware
Data Anomalies
Exploits
Connections

Infection Callbacks
Show Search

Date & Time	URL/Domain	Destination IP	Action
06/30/2015 2:46 AM	kernel-panic.eu/services/images/dev/*	156.153.226.92	Blocked
06/30/2015 3:26 AM	oywtieeicse.com/html/*	156.153.226.92	Blocked
06/30/2015 3:45 AM	zerro03.co.cc	156.153.226.92	Blocked
06/30/2015 3:56 AM	alessandrofalcone.com/images	156.153.226.92	Blocked
06/30/2015 4:16 AM	elleamoda.it/e.exe	156.153.226.92	Blocked
06/30/2015 5:06 AM	report.3179g1iqg179317uo1.com	156.153.226.92	Blocked
06/30/2015 5:26 AM	bronetbro.com	156.153.226.92	Blocked
06/30/2015 6:26 AM	qecipzed.ru/nothin2.exe	156.153.226.92	Blocked
06/30/2015 6:56 AM	vperedzaddos.com	156.153.226.92	Blocked
06/30/2015 7:06 AM	woozgvuqwpqrqn.biz/forum	156.153.226.92	Blocked

Previous
Next

Callback Destination IPs

Close

Behavioral Sandboxing

Defends against polymorphic malware

Solely relying on AV scanners or signature-based monitoring to prevent malware is no longer effective. Today's threats are polymorphic and capable of continually morphing to evade signature-based detection. The iboss Secure Web GatewayPlatform includes a behavior-based approach to malware detection, which doesn't rely on signatures to stop advanced threats.

Dashboard

FireSphere

History: Malware Analysis for 5089c1fb58f3b186a7e2c8de8ef84c7260ffa3b154a163e4a1b9eaa819d4423e

Malware Analysis for Signature 5089c1fb58f3b186a7e2c8de8ef84c7260ffa3b154a163e4a1b9eaa819d4423e

Scan Date:	2015-06-30 14:26:39
Verdict:	Suspicious
Type:	ZIP
Size:	19127
SHA1:	420cf29dab53a2ba68eb62875da7a2e5b15aa64e
SHA256:	5089c1fb58f3b186a7e2c8de8ef84c7260ffa3b154a163e4a1b9eaa819d4423e
MD5:	5810757aff7c45aa35a84e86f5df6261
Total Scan Engines:	55
Positive Malware Verdicts:	1

Engine	Result	Version	Last Scan...
Bkav		1.3.0.6979	06/30/2015
MicroWorl...		12.0.250.0	06/30/2015
nProtect		2015-06-30...	06/30/2015
CAT-Quick...		14.00	06/30/2015
ALYac		1.0.1.4	06/30/2015
Malwareby...		2.1.1.1115	06/30/2015
Zillya		2.0.0.2259	06/30/2015
AegisLab		1.5	06/30/2015
TheHacker		6.8.0.5.584	06/30/2015
BitDefender		7.2	06/30/2015

Behavioral Analysis for File Signature 5089c1fb58 [...]

Summary	Mutexes	Files	Window Info	Network Info	Process Info	Registry Keys	Runtime DLLs	Service Info
---------	---------	-------	-------------	--------------	--------------	---------------	--------------	--------------

Behavioral Analysis Overview

Magic literal:	Zip archive data, at least v2.0 to extract
TrID:	ZIP compressed archive (100.0%)

Close

Detect and contain protocol-evasive threats

Stops advanced malware using hidden protocols like TOR

Advanced malware integrating with the TOR network to circumvent your security represents a pervasive, new class of threat that standard solutions can't see. The method of monitoring good-behaving protocols is not enough and can lead to infections entering the network faster and staying undetected longer. Only iboss monitors the bad-behaving protocols to pinpoint the infection quickly, issue alerts and auto-contain your data to stop loss.

Web Categories

Applications

Evasive Protocols

Browser & OS

Social Media

Allow List

Block List

Keywords

Bandwidth Shaping

Ports

Content / MIME

File Extensions

Domain Extensions

Sleep Schedule

Monitoring

Exceptions

URL Lookup

Preferences

Groups

Tools

Network

Firmware

Subscription

Support

High-Risk Activity Device Lock

WARNING! ALL internet access will be blocked for the violating IP for the configured lock period. A lock to an IP that represents a NATed segment will result in the entire segment being blocked.

To manually unlock the computer navigate to Groups→ Dynamic Computers→ then, click the Unlock icon under the Actions column.

BYOD
Recommended

Enable Tor activity lock

NO

Enable Hot Spot activity lock

NO

Enable Open Door activity lock

NO

Enable Snapchat activity lock

NO

Enable OpenSSL activity lock

NO

Enable UltraSurf activity lock

NO

Enable YouTube activity lock

NO

Send email alert

NO

Enable OpenVPN activity lock

NO

Enable Spot Flux activity lock

NO

Enable BitTorrent activity lock

NO

Lock computer

3

Minutes

Additional Settings

Block SSH / Secure Shell Access

NO

Block RDP/ Remote Desktop Access

NO

Block Incoming FTP Traffic

NO

Block Outgoing FTP Traffic

NO

Block Ping (ICMP)

NO

Dynamic Proxy Blocking(Glype)

NO

Block SSL on Non-standard Ports

YES

Block Rogue Encrypted Connections

YES

SSL Domain Enforcement

YES

Reverse DNS Lookup Support

YES

Block Newsgroups

NO

Block Internal Servers

Disabled

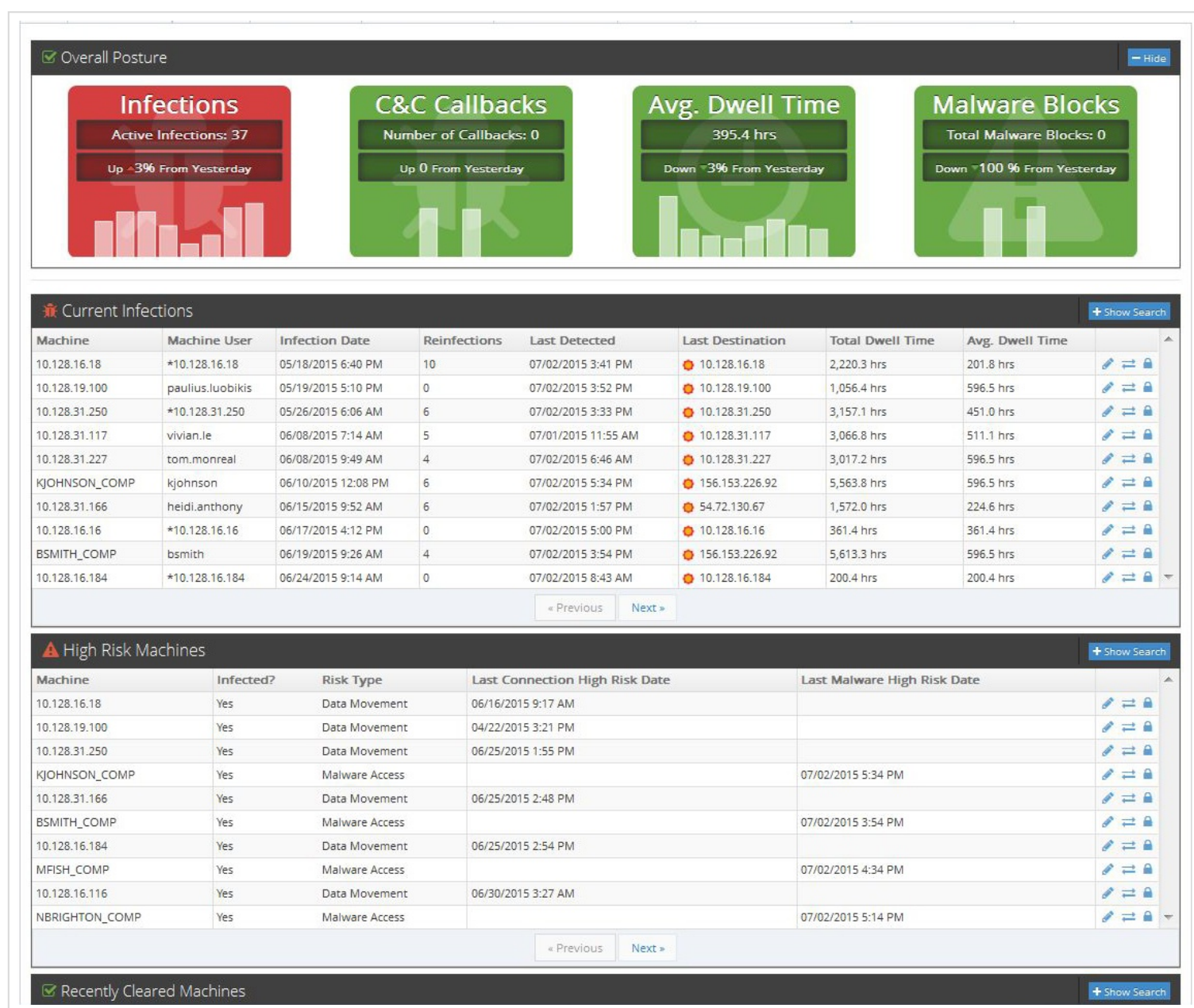
Logging

YES

CISO Command Center

Identify data breaches faster

Deal with incidents not noisy event logs. The iboss Secure Web Gateway Platform automatically consolidates and prioritizes events, translating them into actionable incidents. This not only shortens investigative response time, it reduces data loss when breaches occur. C&C callback monitoring, continuous network anomaly monitoring and behavioral analysis provide an unmatched approach that exposes malware in real-time.



Unified Cloud Platform

Delivers anytime, anywhere security

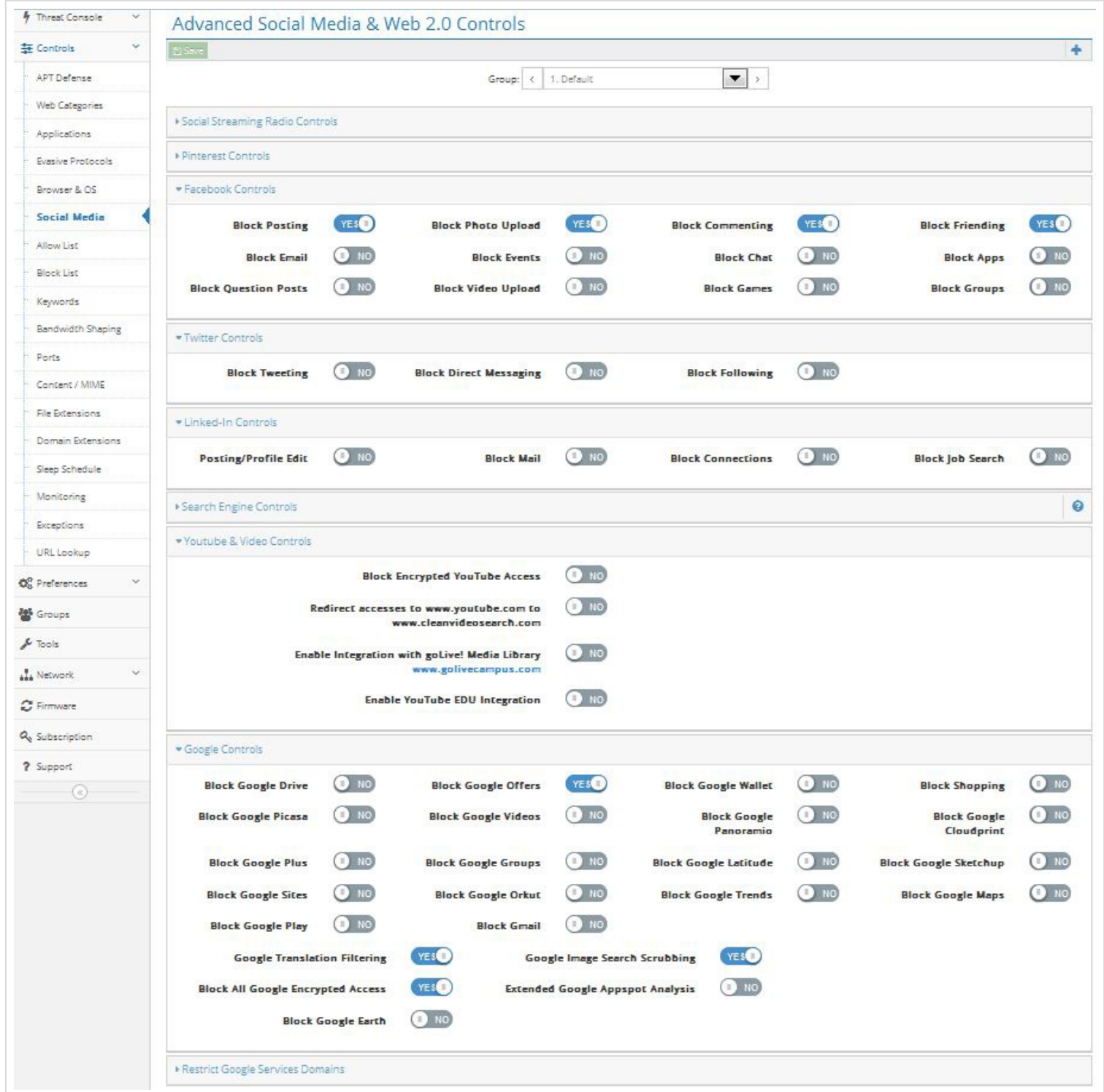
Flexible security across any device, anywhere, and at any time is delivered via iboss Unified Cloud Platform. iboss intelligent cloud architecture ensures you'll never have to backhaul data from remote locations or mobile devices to corporate HQ. Instead, get instant access to the data you need, while maintaining wire-speed performance at your core sites.



Manage Cloud Apps and Social Media

Granular control that stops advanced threats

Many of the applications we rely on to conduct business, such as Skype, WebEx and others, use proprietary signatures and non-standard ports to communicate, but this can introduce threats that result in data loss. In addition, social media apps such as Facebook can be a boon to businesses but unmanaged access introduces risk. The iboss Secure Web Gateway Platform protects you with granular application visibility and control across all 131K ports on your network to defend against advanced threats and misuse, without affecting user experience.



Auto-quarantine high-risk users

Stop the spread of infections

The number of mobile devices, remote locations and roaming users accessing your network has created new sources of advanced threats for which you must be prepared. The iboss Secure Web Gateway Platform employs network-wide scanning to pinpoint high-risk machines and users and quarantine them

to stop the spread of infection, alert you and enable remediation.

The screenshot displays the configuration interface of the iboss Threat Isolator. On the left is a sidebar menu with various settings categories. The main content area is divided into two sections: 'High-Risk Activity Device Lock' and 'Additional Settings'.

High-Risk Activity Device Lock Section:

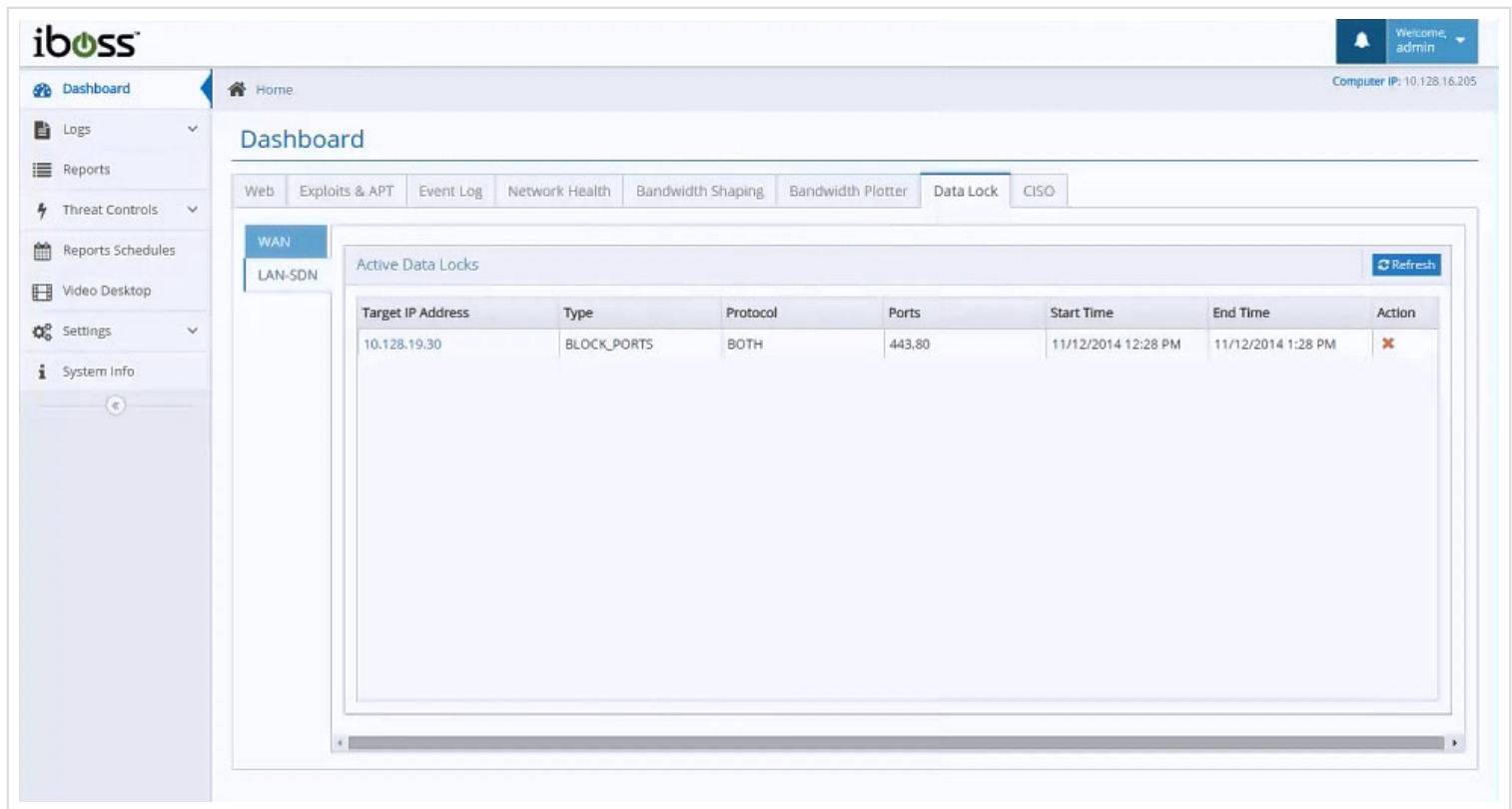
- Warning:** A red warning icon and text state: "WARNING! ALL internet access will be blocked for the violating IP for the configured lock period. A lock to an IP that represents a NATed segment will result in the entire segment being blocked." Below this, instructions read: "To manually unlock the computer navigate to Groups--> Dynamic Computers--> then, click the Unlock icon under the Actions column."
- BYOD (Recommended)** icon.
- Activity Locks:** A grid of toggle switches for various activities, all currently set to 'NO':
 - Enable Tor activity lock
 - Enable Hot Spot activity lock
 - Enable Open Door activity lock
 - Enable Snapchat activity lock
 - Enable OpenSSL activity lock
 - Enable Ultrasurf activity lock
 - Enable YouTube activity lock
 - Send email alert
 - Enable OpenVPN activity lock
 - Enable Spot Flux activity lock
 - Enable BitTorrent activity lock
- Lock computer:** A dropdown menu set to '3' with the unit 'Minutes'.

Additional Settings Section:

- Block SSH / Secure Shell Access:** NO
- Block RDP/ Remote Desktop Access:** NO
- Block Incoming FTP Traffic:** NO
- Block Outgoing FTP Traffic:** NO
- Block Ping (ICMP):** NO
- Dynamic Proxy Blocking(Glype):** NO
- Block SSL on Non-standard Ports:** YES
- Block Rogue Encrypted Connections:** YES
- SSL Domain Enforcement:** YES
- Reverse DNS Lookup Support:** YES
- Block Newsgroups:** NO
- Block Internal Servers:** Disabled
- Logging:** YES

Quarantine internal outbreaks
With iboss Threat Isolator

iboss Threat Isolator puts data protection tools inside the network perimeter for comprehensive protection against exploits such as CryptoLocker or C&C callbacks. It dynamically isolates and contains infections by blocking internal communications between computers on your network. You receive alerts, when a problem is identified, giving you time to remediate and avoid further infection.



Manage SSL and Encrypted Communications

Granular policy enforcement and malware defense

Analysts predict that SSL will comprise 70% of all Internet traffic by 2017. Enforcing encryption policies while trying to detect malware hidden inside SSL traffic can create a conundrum that risks your organization's security. The iboss Secure Web Gateway Platform ensures compliance and protection across all HTTP and HTTPS traffic, with flexible tools in a highly scalable solution.

Gateway SSL Decryption

Actions ▾

Generate SSL Decryption Certificate

+

▸ General Settings

?

▸ User SSL Decryption Alert

?

▸ SSL Decryption Ip Address Bypass

?

▸ Selective SSL Decryption

?

▸ Advanced Selective SSL Decryption

?

▸ Additional SSL Decryption DNS Servers

?

▸ SSL Decryption Certificate

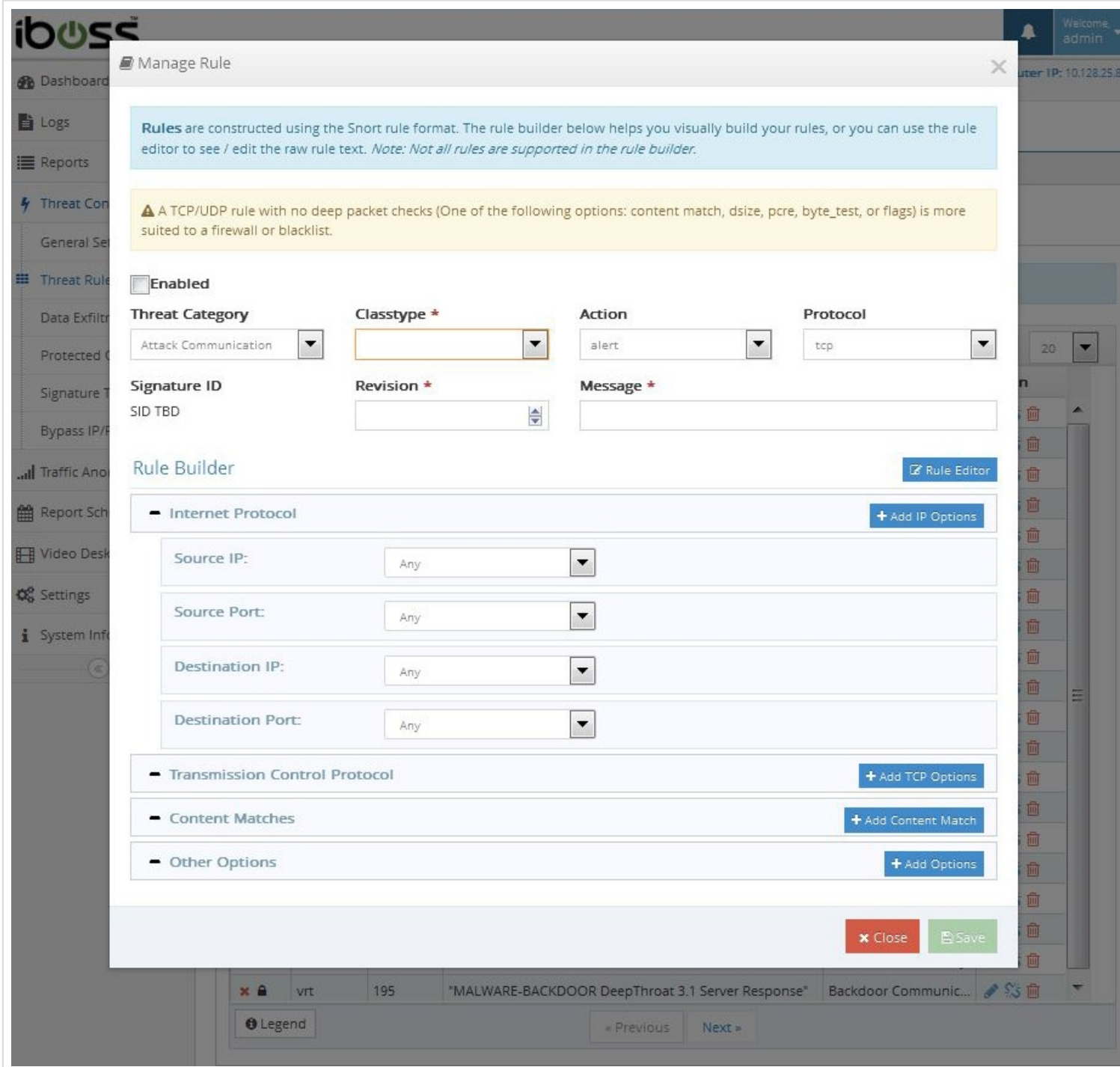
Intelligent Bandwidth Management

Maintain network health and performance

Unlike stateful shaping that continuously applies policy, used by most standard security solutions, iboss smart, stream-based approach allows you to provide uninterrupted bandwidth availability during saturation periods, giving your users more access to technology without compromising performance.

Prevent intrusions with visual IPS tools that simplify rules

Legacy IPS tools rely heavily on manual rule editing which is not only complex, but also time-consuming. With the iboss Secure Web Gateway Platform, creating, managing and editing rules is fast, easy-to-understand and free from errors. The results are more efficiency, less strain on IT resources and lower TCO.



Fast Google-like Log Searches

Search logs faster

Whether you're searching through logs spanning one day or five years, across one gigabyte or multiple petabytes, the iboss Secure Web Gateway Platform delivers your results immediately, without the protracted wait times of competitive solutions. This Google-like capability is enabled by iboss' exclusive dynamic indexing, which ensures the data you need is delivered instantly.

Home > Logs > Web

Error! Please check the settings!

Computer IP: 10.128.25.80

Logs

Actions

Hide Search

Gateway: All Servers

Create Log Report

20

URL Archive

iboss Indexed Search Enabled.

Start Date

07/02/2015

Start Time

12:00 AM

End Date

End Time

11:59 PM

Username

Group

URL/Keyword

* for wildcard

Computer MAC

Computer Name

Location

Source IP

Destination IP

Category

All Categories

Action

All

Audit Event:

All

Report Group

All

Type

URL

Description

* for wildcard

Callout Only

YES

Search

Clear Filters

Date & Time	User	Source IP	URL/Domain	Destination IP	Group	Category	Action
07/02/2015 5:54 PM	jdoe	10.128.16.110	circumvent	156.153.226.92			Blocked
07/02/2015 5:54 PM	jdoe	10.128.16.110	expunge	156.153.226.92			Blocked
07/02/2015 5:44 PM	nbrighton	10.128.16.113	virgin	156.153.226.92			Blocked
07/02/2015 5:44 PM	nbrighton	10.128.16.113	proxy	156.153.226.92			Blocked
07/02/2015 5:44 PM	nbrighton	10.128.16.113	barbital	156.153.226.92			Blocked
07/02/2015 5:34 PM	kjohnson	10.128.16.97	virgin	156.153.226.92			Blocked
07/02/2015 5:34 PM	kjohnson	10.128.16.97	proxy	156.153.226.92			Blocked
07/02/2015 5:34 PM	kjohnson	10.128.16.97	counterfeiting	156.153.226.92			Blocked
07/02/2015 5:24 PM	kjohnson	10.128.16.97	porn	156.153.226.92			Blocked
07/02/2015 5:24 PM	kjohnson	10.128.16.97	prox	156.153.226.92			Blocked
07/02/2015 5:24 PM	kjohnson	10.128.16.97	dimethyltryptamine	156.153.226.92			Blocked
07/02/2015 5:14 PM	nbrighton	10.128.16.113	proxy	156.153.226.92			Blocked
07/02/2015 5:14 PM	nbrighton	10.128.16.113	Cannabis	156.153.226.92			Blocked
07/02/2015 5:14 PM	nbrighton	10.128.16.113	porn	156.153.226.92			Blocked
07/02/2015 5:04 PM	jdoe	10.128.16.110	proxy	156.153.226.92			Blocked

Extend security to WiFi and BYOD

Extend compliance and threat protection

Automatically secure WIFI networks to extend compliance while protecting against advanced threats. Easily integrate guest users via their own Google account, using OAuth or seamlessly integrate with your existing Network Access Controller (NAC).

The screenshot shows the iboss web dashboard. The top right corner displays 'Filtering Enabled' and 'Welcome, admin'. The breadcrumb trail is 'Home > Network > BYOD'. The left sidebar contains a menu with 'Dashboard', 'Threat Console', 'Controls', 'Preferences', 'Groups', 'Tools', 'Network' (selected), 'Internet', 'SSL Decryption', 'SSL Certificates', 'Bandwidth Tracking', 'BYOD' (highlighted), 'LDAP Settings', 'AD & Proxy', 'AD Plugin', and 'Mobile Client'. The main content area is titled 'BYOD Settings' and shows 'General Settings'. The settings include: 'Enable BYOD Web Login' (YES), 'User Inactivity Timeout' (0), 'Custom Mobile Login Page' (http://10.128.16.1), and 'Use Encryption On Mobile Login' (NO). A 'Save' button is at the bottom left of the settings area. The top right of the main area shows 'Computer IP: 10.128.25.80' and 'Current Group: No Filtering'.

MobileEther MDM

Manage device-level policies

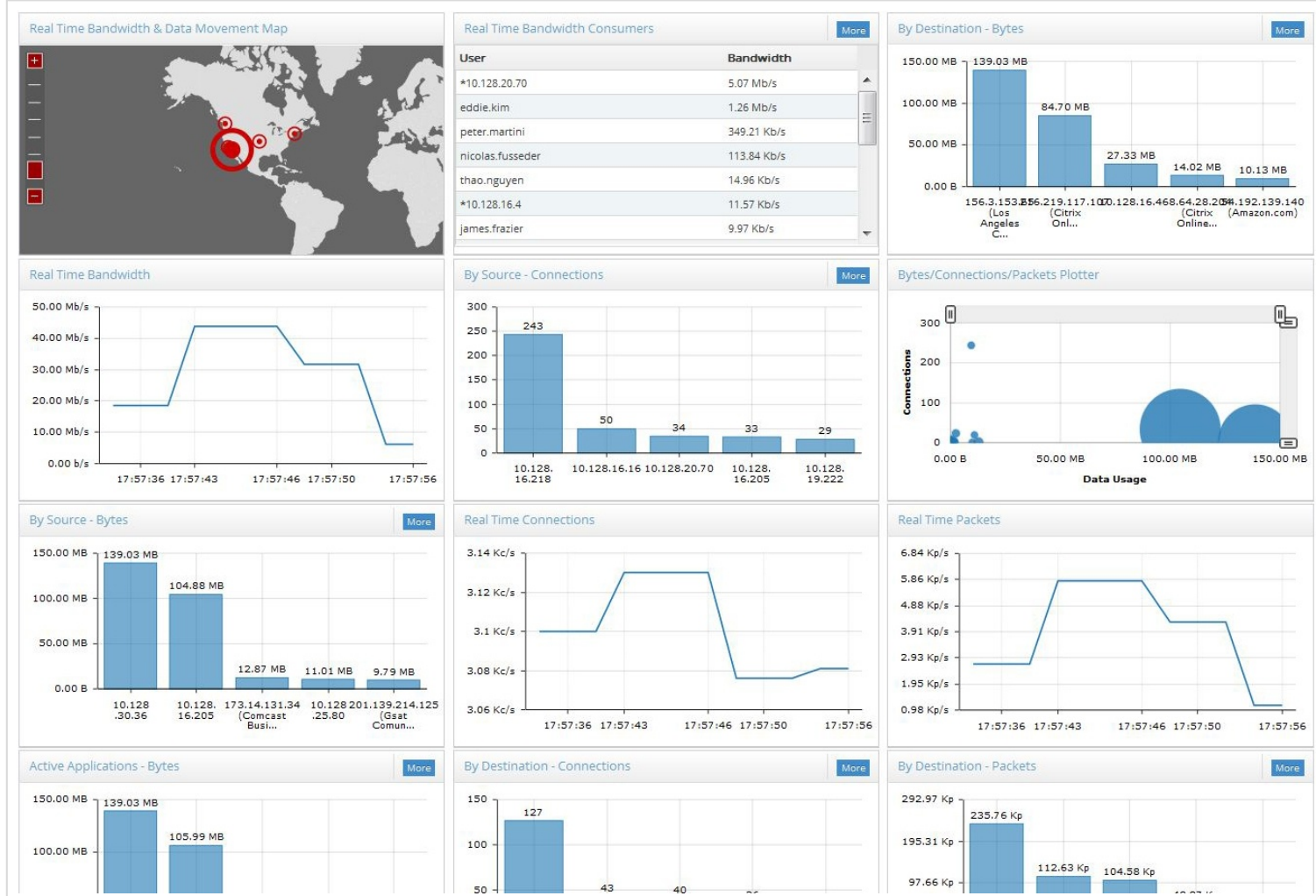
Protect mobile devices and enforce policies with full capabilities from iboss award-winning MDM. Push apps, wipe devices if lost or stolen, and enforce device-level restrictions. Alliances with technology partners such as Apple and Samsung make managing devices a snap.



Threat and Event Console Reporting

Respond and document incidents via responsive interface

The iboss Secure Web Gateway Platform includes a Threat and Event Console reporting that is integrated across all features and is easy to use, with a highly-responsive, intuitive interface, guided interactive wizards, and customizable reporting templates. Within seconds, go from organization-wide visibility, to a 360-degree view of each network user, including Web activity, application use, bandwidth consumption, data loss risks and more.



Blended AV Scanning

Prevents malicious files with info from multiple feeds

iboss AV scanning gets malware feeds from a variety of proprietary and best-of-breed sources including Kaspersky AV, blended C&C feeds, iboss Secure Web Gateway Platform Sandboxing and Baselining, and more. Within minutes these malware feeds are synchronized in the cloud and delivered to the iboss Secure Web Gateway Platform database, whether on-premises or in the cloud.

Web security has evolved beyond traditional URL filtering. The iboss Secure Web Gateway Platform provides next-gen features that include granular management of social media, Google services, and applications, SSL traffic inspection, and comprehensive user-based reporting, centrally managed from a

responsive interface. iboss innovative, advanced malware and APT defense ensure unrivaled protection from today's most sophisticated attacks.

iboss

Dashboard

Threat Console

Controls

APT Defense

Web Categories

Applications

Evasive Protocols

Browser & OS

Social Media

Allow List

Block List

Keywords

Bandwidth Shaping

Ports

Content / MIME

File Extensions

Domain Extensions

Sleep Schedule

Monitoring

Exceptions

URL Lookup

Preferences

Groups

Tools

Network

Firmware

Subscription

Support

Home > Controls > Web Categories

Computer IP: 10.128.23.80
Current Group: No Filtering

Web/SSL Categories

Save

Group: 1. Default

Category Scheduling

Always Block Selected Categories

Block Selected Categories Using an Advanced Schedule

Advanced Scheduling

Additional Settings

Enable Logging

YES

Enable Stealth Mode

NO

Enable Strict Safesearch Enforcement

NO

Enable HTTP Scanning on non-standard ports

NO

Allow Legacy HTTP 1.0 requests

NO

Enable ID Theft / IP Address URL Blocking










































































































YES










































































































Block Uncategorized Sites

NO

Categories

Actions

Category	Actions	Priority
Ads	    	0
Alcohol & Tobacco	    	0
Auctions	    	0
Business	    	2
Dictionary	    	0
Education	    	0
File Sharing	    	0
Food	    	0
Friendship	    	0
Games	    	0
Guns & Weapons	    	0
Image / Video Search	    	0
Malware	    	0
News	    	0
Political	    	0
Porn/Nudity	    	0
Professional Services	    	0
Religion	    	0
Sex Ed	    	0
Sports	    	0
Swimsuit	    	0

Category	Actions	Priority
Adult Content	    	0
Art	    	0
Audio & Video	    	0
Dating & Personals	    	0
Drugs	    	0
Entertainment	    	0
Finance	    	0
Forums	    	0
Gambling	    	0
Government	    	1
Health	    	0
Jobs	    	0
Mobile Phones	    	0
Organizations	    	0
Porn - Child	    	0
Private Websites	    	0
Real Estate	    	0
Search Engines	    	0
Shopping	    	1
Streaming Radio/TV	    	0
Technology	    	0

Integration via Restful API

Easy integration with partner ecosystems

The convergence of mobile, applications and cloud technologies has made the easy integration of security tools an imperative. The iboss Secure Web Gateway Platform includes an open partner ecosystem via RESTFUL API for streamlined integration that enables optimum performance.



Ready to see the iboss Secure Web Gateway Platform in Action?

[Request Demo\(/demo-request\)](/demo-request)

The iboss Story

[About Us\(/about-us\)](/about-us)

[Leadership\(/leadership\)](/leadership)

[Board\(/board-of-directors\)](/board-of-directors)

[Blog\(/blog.iboss.com\)](//blog.iboss.com)

[In the News\(/in-the-news\)](/in-the-news)

[Press Releases\(/press-releases\)](/press-releases)

Legal

[Privacy Policy\(/privacy-policy\)](/privacy-policy)

[Terms of Use\(/terms-of-use\)](/terms-of-use)

[Acceptable Use Policy\(/acceptable-use-policy\)](/acceptable-use-policy)

Site Map

[Site Map\(/site-map\)](/site-map)

Learn iboss

[iboss University Overview\(/iboss-university\)](/iboss-university)

[ISCP Certification\(/www.iboss.com/iuniversity-iscp\)](//www.iboss.com/iuniversity-iscp)

[Expand Your Knowledge\(/www.iboss.com/iuniversity-eyk\)](//www.iboss.com/iuniversity-eyk)

Contact Support

[Support Overview\(/support\)](/support)

[Open a Ticket\(http://support.iboss.com\)](http://support.iboss.com)

Activate iboss Pro([//www.iboss.com/phantomweb/action/activation/selectProduct?b=1](http://www.iboss.com/phantomweb/action/activation/selectProduct?b=1))
Cloud Management([//www.iboss.com/phantomweb/action/enterprisemanagement/login](http://www.iboss.com/phantomweb/action/enterprisemanagement/login))

North America:

☎ 877-742-6832 X3

International:

☎ 858-568-7051 X3

☎ Contact Sales

Request Demo([//www.iboss.com/demo-request](http://www.iboss.com/demo-request))

Request Evaluation([//www.iboss.com/eval-request](http://www.iboss.com/eval-request))

Request Information([//www.iboss.com/info-request](http://www.iboss.com/info-request))

North America:

☎ 877-742-6832 X1

Contact local distributor or:

✉ sales@iboss.com(mailto:sales@iboss.com)

International:

☎ 858-568-7051 X1

Contact local distributor or:

✉ sales@iboss.com(mailto:sales@iboss.com)

EMEIA:

☎ +44 (0) 203 713 0471

Contact local distributor or:

✉ emeia@iboss.com(mailto:emeia@iboss.com)